Monitoring Bluecoat Antivirus

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Blue Coat AV prevents viruses, trojans, worms, and spyware from entering your organization via the Web. Gateway anti-virus scanning secures rogue channels such as personal Web email and Web downloads.

This means that if the Bluecoat AV malfunctions, it can expose your mission-critical environment to malicious virus attacks that can cause significant data loss. To prevent this, the Bluecoat AV has to be monitored at all times. This what eg Enterprise exactly does.

Chapter 2: How to Monitor Bluecoat AntiVirus Using eG Enterprise?

eG Enterprise monitors the Bluecoat AntiVirus in an agentless manner. All that is required for this is a single eG agent on any remote Windows host in the environment. This agent is capable of monitoring the performance of the Bluecoat AntiVirus by polling the SNMP MIB of the Bluecoat AntiVirus. To enable the eG agent to communicate with the Bluecoat AntiVirus and collect performance metrics, a set of pre-requisites should be fulfilled. These requirements are provided below.

2.1 Pre-requisites for Monitoring the Bluecoat AntiVirus

To enable the eG agent to collect performance metrics from a Bluecoat AntiVirus, the following pre-requisites should be fulfilled:

- The Bluecoat AntiVirus should be SNMP-enabled.
- The eG agent should be able to access the target Bluecoat AntiVirus over the network.

Once the pre-requisites are fulfilled, add and configure the Bluecoat AntiVirus component to work with eG agent to start monitoring the component. The steps for achieving this are explained below.

2.2 Managing the Bluecoat AntiVirus

The eG Enterprise cannot automatically discover the Bluecoat AntiVirus so that you need to manually add the component for monitoring. To manage a Bluecoat AntiVirus component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the Infrastructure tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select *Bluecoat AntiVirus* as the **Component type**. Then, click the **Add New Component** button. This will invoke Chapter 2.

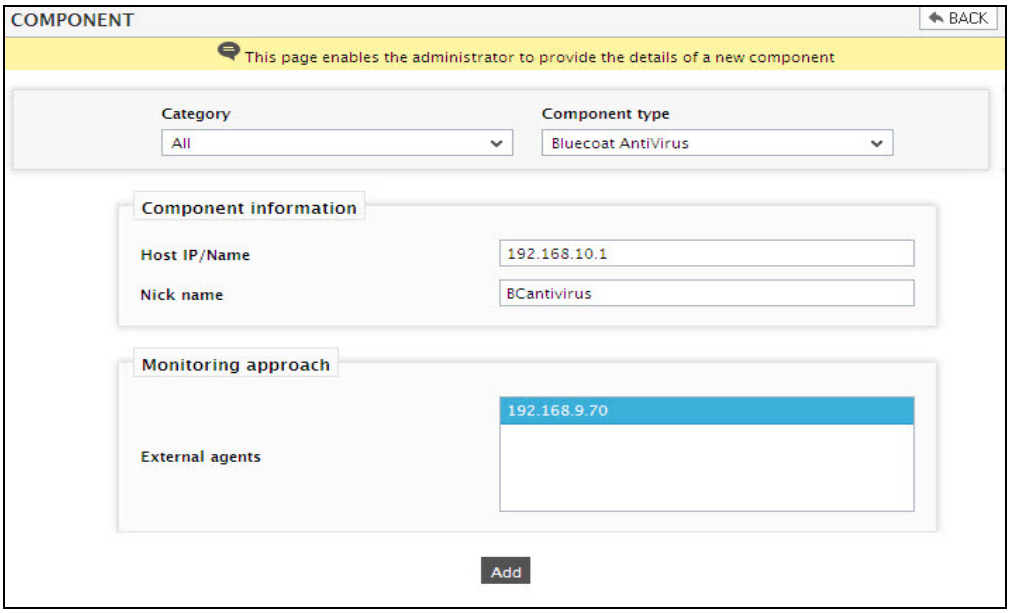

Figure 2.1: Adding a new Bluecoat AntiVirus component

4. Specify the details of **Host IP** and **Nick name** of the Bluecoat AntiVirus and click the **Add** button to add the new component.
5. The Bluecoat AntiVirus so added will be managed automatically by eG Enterprise. Then, try to sigout of the eG administrative interface. This will bring up Figure 2.2, where you can view the complete list of unconfigured tests for the added Bluecoat AntiVirus component.

Figure 2.2: Viewing the list of unconfigured tests for the Bluecoat Antivirus

6. Click on any test in the list of unconfigured tests. For instance, click on the **Antivirus Scan Status** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.

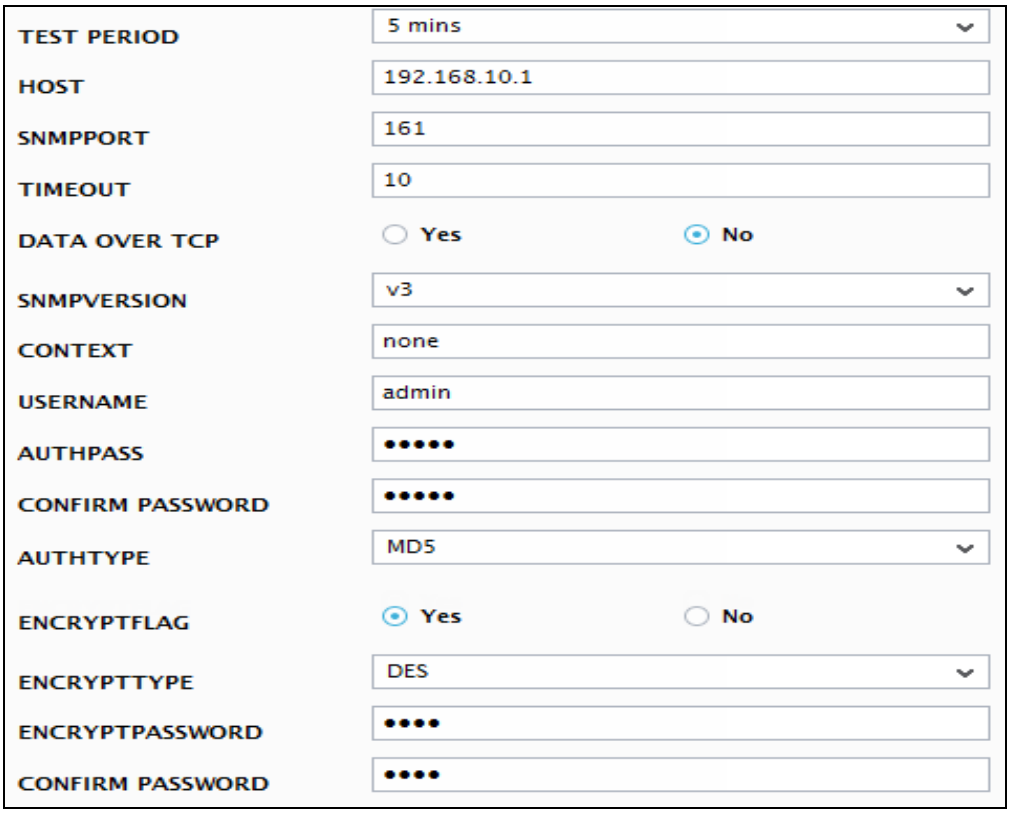

Figure 2.3: Configuring the Antivirus Scan Status test

7. To know how to configure parameters, refer to **Monitoring the Bluecoat AV**.
8. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the Bluecoat AV

eG Enterprise presents 100% web-based *Bluecoat AntiVirus* monitoring model that can promptly alert you to a sudden non-availability of the anti-virus or excessive resource usage by the anti-virus.

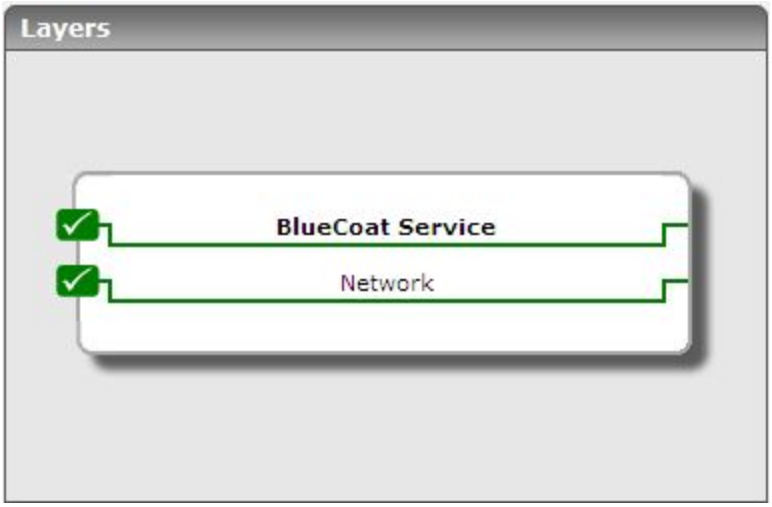

Figure 3.1: Layer model of Bluecoat AV

Each layer of Figure 1.1 is mapped to a set of tests that reports a variety of metrics that can provide accurate answers to the following performance queries:

- Is Bluecoat AV available over the network?
- Have any infected files been detected?
- Is the Bluecoat AV utilizing resources excessively? If so, which resource is it?

3.1 The Network Layer

This layer monitors the availability of the Bluecoat AV over the network, and alerts you to bad network connections (if any) to the anti-virus.

Figure 3.2: The test mapped to he Network layer

Since this test has been dealt with elaborately in the *Monitoring Windows and Unix Servers* document, let us proceed to the next layer.

3.2 The Bluecoat Service Layer

This layer measures the overall efficiency of the Bluecoat AV in isolating virus infected files, and also reveals how resource-efficient the anti-virus is.

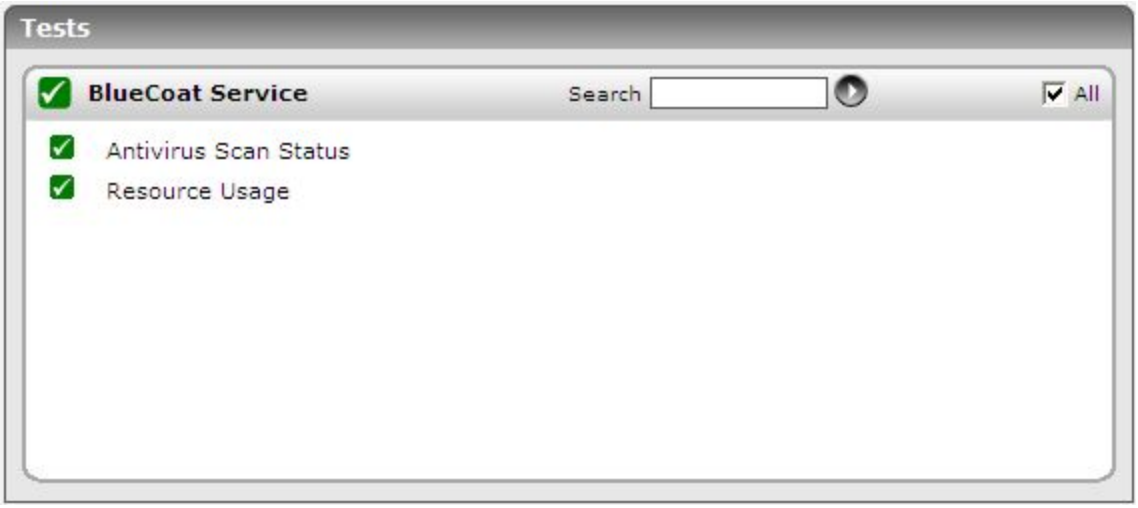

Figure 3.3: The test mapped to the BlueCoat Service layer

3.2.1 Antivirus Scan Status Test

This test measures the effectiveness of the Bluecoat AV software in isolating file infections.

Target of the test : A Bluecoat AV

Agent deploying the test : A remote agent

Outputs of the test : One set of results for Bluecoat AV being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This

Parameter	Description
	parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Number of files scanned	Indicates the number of files scanned by Bluecoat AV for virus attacks.	Number	
Number of files infected	Indicates the number of files infected.	Number	Ideally, the value of this measure should be 0. A non-zero value indicates the existence of one/more viruses on the target host.

3.2.2 Resource Usage Test

This test reveals whether the Bluecoat AV is utilizing each of the resources available to it optimally.

Target of the test : A Bluecoat AV

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each resource available to the Bluecoat AV.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote

Parameter	Description
	SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard

Parameter	Description
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Resource usage	Indicates the status of usage of this resource.		The states reported by this measure and the numeric values that correspond to the states are as follows: State: Normal – Numeric Value: 1 State: Usage High – Numeric Value: 2 **Note:** By default, this measure reports the **State**s listed in the table above to indicate the status of a resource. The graph of this measure however, represents the status using the numeric equivalents - 1 or 2.
Resource utilization	Indicates the percent utilization of this resource.	Percent	A high value is indicative of excessive utilization of the corresponding resource. For instance, if the resource is 'CPU', then a high value indicates high CPU usage.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.